Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of:	)	
	)	
Communications Assistance for	)	CC Docket No. 97-213
Law Enforcement Act	)	
	)	

THIRD REPORT AND ORDER

Adopted: August 26, 1999 **Released: August 31, 1999**

By the Commission:

TABLE OF CONTENTS

I. INTRODUCTION

1. In this *Third Report and Order* (*Third R&O*), the Commission adopts technical requirements for wireline, cellular, and broadband Personal Communications Services (PCS) carriers to comply with the assistance capability requirements prescribed by the Communications Assistance for Law Enforcement Act of 1994 (CALEA, or the Act).[1] Specifically, we require that all capabilities of J-STD-025 (interim standard) and six of nine "punch list" capabilities requested by the Department of Justice (DoJ)/Federal Bureau of Investigation (FBI) be implemented by wireline, cellular, and broadband PCS carriers. While we are requiring that a packet-mode capability be implemented by such carriers, we are not at this time adopting technical requirements for packet-mode communications, but will permit packet-mode data to be delivered to law enforcement under the interim standard, discussed below, pending further study of packet-mode communications by the telecommunications industry.

II. BACKGROUND

2. CALEA, enacted on October 25, 1994, was intended to preserve the ability of law enforcement officials to conduct electronic surveillance effectively and efficiently in the face of rapid advances in telecommunications technology.[2] In enacting this statute, however, Congress

[1] Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended in 18 U.S.C. § 2522, and 47 U.S.C. §§ 229, 1001-1010).

[2] 140 Cong. Rec. H-10779 (daily ed. October 7, 1994) (statement of Rep. Hyde).

recognized the need to protect privacy interests within the context of court- authorized electronic surveillance. Thus, in defining the terms and requirements of the Act, Congress sought to balance three important policies: "(1) to preserve a narrowly focused capability for law enforcement agencies to carry out properly authorized intercepts; (2) to protect privacy in the face of increasingly powerful and personally revealing technologies; and (3) to avoid impeding the development of new communications services and technologies."[3]

3. Section 103 of CALEA establishes four general "assistance capability requirements" that carriers must meet to achieve compliance with CALEA.[4] Section 103(a) requires that a telecommunications carrier shall ensure that its equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of:

> (1) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to intercept, to the exclusion of any other communications, all wire and electronic communications carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber of such carrier concurrently with their transmission to or from the subscriber's equipment, facility, or service, or at such later time as may be acceptable to the government;
>
> (2) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to access call-identifying information[5] that is reasonably available[6] to the carrier--
>
> > (A) before, during, or immediately after the transmission of a wire or electronic communication (or at such later time as may be acceptable to the government); and

---

[3] H.R. Rep. No. 103-827, 103d Cong., 2d Sess., pt. 1, at 13 (1994). A more detailed discussion of CALEA can be found in the *Further Notice of Proposed Rule Making* (*Further NPRM*) in this proceeding, 13 FCC Rcd 22632 (1998), at ¶¶ 3-10.

[4] *See* section 103(a)(1)-(4) of CALEA, 47 U.S.C. § 1002(a)(1)-(4).

[5] Section 102(2) of CALEA defines "call-identifying information" as "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier." 47 U.S.C. § 1001(2).

[6] The Act does not define or interpret the term "reasonably available." Accordingly, the *Further NPRM* requested comment on what factors should be used by the Commission in determining whether call-identifying information is reasonably available. *See Further NPRM*, at ¶ 25.

> (B) in a manner that allows it to be associated with the communication to which it pertains,
>
> except that, with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127 of title 18, United States Code), such call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number);
>
> (3) delivering intercepted communications and call-identifying information to the government, pursuant to a court order or other lawful authorization, in a format such that they may be transmitted by means of equipment, facilities, or services procured by the government to a location other than the premises of the carrier; and
>
> (4) facilitating authorized communications interceptions and access to call-identifying information unobtrusively and with a minimum of interference with any subscriber's telecommunications service and in a manner that protects--
>
> (A) the privacy and security of communications and call-identifying information not authorized to be intercepted; and
>
> (B) information regarding the government's interception of communications and access to call-identifying information.

4. Section 107(a)(2) of CALEA contains a "safe harbor" provision, stating that "[a] telecommunications carrier shall be found to be in compliance with the assistance capability requirements under section 103, and a manufacturer of telecommunications transmission or switching equipment or a provider of telecommunications support services shall be found to be in compliance with section 106, if the carrier, manufacturer, or support service provider is in compliance with publicly available technical requirements or standards adopted by an industry association or standard-setting organization, or by the Commission under subsection (b), to meet the requirements of section 103."[7] Section 107(b) authorizes the Commission, upon petition, to establish rules, technical requirements or standards necessary for implementing section 103 "[i]f

[7] 47 U.S.C. § 1006(a)(2). We note, however, that individual carriers are free to choose any technical solution that meets the assistance capability requirements of CALEA, whether based on an industry standard or not. Carriers, therefore, have some degree of flexibility in deciding how they will comply with CALEA's section 103 requirements. See H.R.Rep. No.103-827, 103rd Cong., 2d Sess, pt. 1, at 3507 (1994)("Compliance with the industry standard is voluntary not compulsory. Carriers can adopt other solutions for complying with the capability requirements.")

industry associations or standard-setting organizations fail to issue technical requirements or standards or if a Government agency or any other person believes that such requirements or standards are deficient."[8]

5. Subcommittee TR45.2 of the Telecommunications Industry Association (TIA) developed the interim standard to serve as a "safe harbor" for wireline, cellular, and broadband PCS carriers and manufacturers under section 107(a) of CALEA.[9] That standard defines services and features required by wireline, cellular, and broadband PCS carriers to support lawfully authorized electronic surveillance, and specifies interfaces necessary to deliver intercepted communications and call-identifying information to a law enforcement agency (LEA).[10] Several parties filed petitions for rulemaking with the Commission, pursuant to section 107(b) of CALEA, contending that the interim standard was either overinclusive or underinclusive. Specifically, DoJ/FBI argue that the interim standard is underinclusive and does not satisfy CALEA requirements because it fails to include the following nine essential capabilities:

> 1) Content of subject-initiated conference calls -- Capability would enable law enforcement to access the content of conference calls supported by the subject's service (including the call content of parties on hold).[11]

[8] 47 U.S.C. § 1006(b).

[9] 47 U.S.C. § 1006(a). This section states that telecommunications carriers and manufacturers are deemed CALEA-compliant if they meet publicly available standards adopted by industry or the Commission.

[10] The interim standard was jointly published in December 1997 by TIA and Committee T1, sponsored by the Alliance for Telecommunications Industry Solutions, as J-STD-025, *Lawfully Authorized Electronic Surveillance*. A more detailed discussion of the development of the interim standard can be found in the *Further NPRM*, at ¶¶ 11-15.

[11] We note that confusion may arise over the terms "subscriber" and "subject." At pp. 27-28 of their March 27, 1998 Joint Petition for Expedited Rulemaking, DoJ/FBI define these terms as follows:

> When we refer to "subscriber," we are referring to the person or entity whose "equipment, facilities, or services" (47 U.S.C. § 1002(a)(1)) are the subject of an authorized law enforcement surveillance activity. The subscriber often will be a person or entity suspected of criminal activity, but in some instances, the subscriber will simply be someone whose relationship to a suspected criminal (e.g., spouse or employer) makes it likely that criminal activity will be transacted or discussed over the subscriber's facilities. When we refer to "intercept subject" or "subject," we are referring to any person who is using the subscriber's equipment, facilities, or services, and whose conversations (or dialing activity) therefore would be capable of being acquired during an interception. In a particular investigation, the "intercept subjects" could include the subscriber, who may or may not be involved in criminal activity; a non-subscriber who is not involved in criminal activity; or a non-subscriber who *is* involved in criminal activity.

2) Party hold, join, drop -- Messages would be sent to law enforcement that identify the active parties of a call. Specifically, on a conference call, these messages would indicate whether a party is on hold, has joined or has been dropped from the conference call.

3) Subject-initiated dialing and signaling information -- Capability would provide a LEA access to all dialing and signaling information available from the subject would inform law enforcement of a subject's use of features (such as the use of flash-hook and other feature keys).

4) In-band and out-of-band signaling (notification message) -- A message would be sent to a LEA whenever a subject's service sends a tone or other network message to the subject or associate (e.g., notification that a line is ringing or busy).

5) Timing information -- Information necessary to correlate call-identifying information with the call content of a communications interception would be sent to a LEA.[12]

6) Surveillance status -- A message that would verify that an interception is still functioning on the appropriate subject would be sent to a LEA.

7) Continuity check tone (c-tone) -- An electronic signal would alert a LEA if the facility used for delivery of call content interception has failed or lost continuity.

8) Feature status -- A message would affirmatively notify a LEA of any changes in features to which a subject subscribes.

9) Dialed digit extraction[13] -- Information sent to a LEA would include those digits dialed by a subject after the initial call setup is completed.

6. The Center for Democracy and Technology (CDT), Electronic Frontier Foundation (EFF), Electronic Privacy Information Center (EPIC), and American Civil Liberties Union (ACLU) argue that the interim standard is overinclusive because it includes location information and packet-mode communications capabilities. Specifically, the interim standard includes a

[12] Delivery within three seconds of the event producing the call-identifying information is requested, together with a time stamp indicating the timing of the event within an accuracy of 100 milliseconds. *See* DoJ/FBI Joint Petition for Expedited Rulemaking, filed March 27, 1998, at 51-52.

[13] This capability has also been referred to as "post-cut-through dialing and signaling."

location parameter that would identify the location of a subject's "mobile terminal" whenever this information is reasonably available at the intercept access point and its delivery to law enforcement is legally authorized. Location information would be available to the LEA irrespective of whether a call content channel (CCC) or a call data channel (CDC) was employed.[14] The interim standard also provides for LEA access to call-identifying information and the interception of wire and electronic telecommunications, regardless of whether the telecommunications are carried in circuit-mode or in packet-mode.[15] The interim standard further states that the "call-identifying information associated with the circuit-mode content surveillance is provided on the [call data channel]," but does not specifically address whether call-identifying information, if any, associated with packet-mode surveillance must be provided over a call data channel.[16]

7. The Commission released a *Further Notice of Proposed Rule Making (Further NPRM)* in this proceeding to address alleged deficiencies in the interim standard. In the *Further NPRM*, we stated that we did not intend to reexamine any of the uncontested technical requirements of the interim standard, but would make determinations only regarding whether the 11 disputed capabilities met the assistance capability requirements specified in section 103 of CALEA.[17]

8. The *Further NPRM* tentatively concluded that the provision by carriers[18] to LEAs of location information and five punch list capabilities is necessary to meet the assistance capability requirements under section 103(a). Those five punch list capabilities are subject-initiated conference calls; party hold, join, drop on conference calls; subject-initiated dialing and signaling information; and timing information. The *Further NPRM* also sought comment on whether the dialed digit extraction (post-cut-through digits) capability is necessary to meet the assistance capability requirements under Section 103(a). The Further NPRM also tentatively concluded that three punch list capabilities--surveillance status, continuity check tone and feature status--were not assistance capability requirements under Section 103(a).

---

[14] J-STD-025 at § 6.4.6, and at §§ 5.4.1-5.4.8, Tables 1, 5, 6, and 8.

[15] *Id.* at §§ 3 and 4.5. Section 3 defines circuit-mode as "a communication using bi-directional paths switched or connected when the communication is established. The entire communication uses the same path." Section 3 defines packet-mode as "a communication where individual packets or virtual circuits of a communication within a physical circuit are switched or routed by the accessing telecommunication system. Each packet may take a different route through the intervening network(s)."

[16] *Id.*

[17] *Further NPRM*, at ¶¶ 44-45.

[18] Hereinafter, reference to "carriers" includes only wireline, cellular and broadband PCS carriers.

9. We emphasized in the *Further NPRM* that we were directed, pursuant to section 107(b) of CALEA, to take into account five factors in our analysis of deficiency petitions brought to our attention.[19] Those factors are: (1) meeting the assistance capability requirements of section 103 by cost-effective methods; (2) protecting the privacy and security of communications not authorized to be intercepted; (3) minimizing the cost of CALEA compliance on residential ratepayers; (4) serving the policy of the United States to encourage the provision of new technologies and services to the public; and, (5) providing a reasonable time and conditions for CALEA compliance.[20]

10. We also tentatively concluded in the *Further NPRM* that, if the additional technical requirements we proposed were adopted, they could be most efficiently implemented by permitting TIA to modify J-STD-025 in accord with our determinations. We stated that although TIA may have to undertake additional work to implement the additional technical requirements identified in the *Further Notice*, it has the experience and resources to develop technical specifications and implement CALEA's requirements most rapidly.[21]

11. Finally, we sought comment in the *Further NPRM* on what role, if any, we can or should play in assisting telecommunications carriers other than wireline, cellular, and broadband PCS to set standards for, or to achieve compliance with, CALEA's requirements.[22]

III. DISCUSSION

A. General Comments

1. Scope of Proceeding

12. We stated in the *Further NPRM* that the uncontested technical requirements of the interim standard are beyond the scope of this proceeding. EPIC, EFF, and ACLU, challenge this tentative conclusion. They argue that our decision to foreclose comment on "uncontested" issues improperly insulates the interim industry standard from public scrutiny, is inconsistent with the

[19] *Further NPRM*, at ¶¶ 29-30.

[20] 47 U.S.C. § 1006(b).

[21] *Further NPRM*, at ¶¶ 132-133.

[22] *Id.* at ¶ 141.

requirements of the Administrative Procedure Act, and undermines the value of our authority over the process that led to the standard.[23]

13. *Discussion.* We find no need to reexamine the entire interim standard. CALEA provides that the Commission establish technical requirements or standards upon being petitioned by a government agency or other person, where industry fails to issue technical requirements or standards or such government agency or person believes the technical requirements or standards are deficient.[24] As discussed in the *Further NPRM*, a draft industry standard was submitted for balloting in spring 1997 to all interested participants under procedures of the American National Standards Institute.[25] Subsequently, petitions for rulemaking were filed with the Commission, pursuant to section 107(b), contending that the interim standard was deficient; however, none of these petitions raised any issue pertaining to the interim standard other than those relating to location information, packet-mode communications, and the DoJ/FBI punch list. Further, on April 20, 1998, our Wireless Telecommunications Bureau and Office of Engineering and Technology issued a *Public Notice* in this proceeding that solicited specific comment on the scope of the assistance capability requirements necessary to satisfy the obligations imposed by CALEA.[26] Again, no deficiencies in the interim standard were identified other than with respect to location information, packet-mode communications, and the punch list. We find that no other issues were raised before the Commission regarding the interim standard. Since section 107(b) requires the Commission to resolve specific disputes raised by petition regarding alleged deficiencies in the industry standard, we decline to consider other aspects of that standard not challenged in this proceeding. Moreover, by focusing only on those specific technical issues properly raised before us, we will achieve greater efficiency and will permit telecommunications manufacturers and carriers to deploy CALEA solutions on a more expedited basis. Accordingly, we find that wireline, cellular, and broadband PCS carriers must comply with all uncontested requirements of the interim industry standard by June 30, 2000.[27]

2. Definition of "Reasonably Available"

14. While the Act defines call-identifying information as "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a

[23] EPIC/EFF/ACLU Comments, at 33-34.

[24] 47 U.S.C. § 1006(b).

[25] *Further NPRM*, at ¶ 12 & n.28.

[26] DA 98-762.

[27] *See* ¶ 36, *infra*.

telecommunications carrier,"[28] it does not define "reasonably available." The *Further NPRM* asked for comment on the factors we should use in determining whether call-identifying information to be provided by a carrier to a LEA is "reasonably available" to the carrier.[29] The interim standard includes a definition of this term which states that call-identifying information is "reasonably available" to a carrier if such information is present at an intercept access point (IAP) for call processing purposes. The IAP is "a point within a telecommunication system where some of the communications or call-identifying information of an intercept subject's equipment, facilities, and services are accessed." There may be one or more IAPs.[30]

15. *Comments.* AT&T and Nextel Communications, Inc. (Nextel) state that they support the definition of reasonably available call-identifying information given in the interim standard.[31] AT&T further states that in the *Further NPRM* we departed from that definition, and that if we affirm the proposals set forth therein, we should acknowledge that processing that takes place entirely within terminal equipment or other subscriber-owned or maintained equipment is not reasonably available.[32]

16. DoJ/FBI contend that the concept of "reasonable availability" is a technical one that focuses on network design, not a financial one involving carrier balance sheets. Further, DoJ/FBI disagree that call-identifying information should be deemed reasonably available to a carrier only if the information is present at an IAP for call processing purposes. DoJ/FBI contend that the interim standard imposes no requirements regarding where or how IAPs are to be situated within a network. Instead, according to DoJ/FBI, the interim standard leaves the choice of IAPs entirely to the discretion of individual carriers and manufacturers and permits a carrier to situate IAPs without regard to the impact on the carrier's ability to expeditiously isolate and enable a LEA to access call-identifying information. DoJ/FBI maintain that it is untenable to take the position, as reflected in the J-STD-025 definition, that there is never any need to modify network protocols, even when the modification would be technically straightforward and would provide

---

[28] 47 U.S.C. § 1001(2).

[29] *Further NPRM*, at ¶ 25.

[30] *See*, respectively, §§ 3 and 4.2.2 of J-STD-025, at 8 and 14.

[31] AT&T Comments, at 3-4 (*citing* J-STD-025 at § 4.2.1); Nextel Comments, at 4. Section 4.2.1 of J-STD-025 is titled "Assumptions," and the last paragraph of p. 13 states: "Call-identifying information is *reasonably available* if the information is present at an Intercept Access Point (IAP) for call processing purposes. Network protocols (except LAESP) do not need to be modified solely for the purpose of passing call-identifying information. The specific elements of call-identifying information that are reasonably available at an IAP may vary between different technologies and may change as technology evolves." [Note: "LAESP" stands for Lawfully Authorized Electronic Surveillance Protocol.]

[32] AT&T Comments, at 6.

access to call-identifying information without imposing significant burdens on the network. Accordingly, DoJ/FBI propose a modified definition of reasonably available call-identifying information, as follows:

> Call-identifying information is reasonably available if (1) it is present in an element in the carrier's network that is used to provide the subscriber with the ability to originate, terminate, or direct communications and (2) it can be accessed there, or can be delivered to an IAP located elsewhere, without unreasonably affecting the call processing capabilities of the network.[33]

17. Nextel contends that we should "validate" the J-STD-025 definition of reasonably available call-identifying information because the objections of DoJ/FBI to that definition are not well-grounded. Nextel states that the interim standard requires IAPs to be placed to access call content and call-identifying information, and that the reason the standard requires that call-identifying information be present at the IAP for call processing purposes is that Congress narrowly defined such information as dialing and signaling information used for the purposes of routing calls through a carrier's network.[34]

18. The Cellular Telecommunications Industry Association (CTIA) maintains that DoJ's/FBI's contention that a carrier may select IAPs that limit LEA collection of call-identifying information is erroneous. CTIA asserts that a carrier that attempted to implement J-STD-025 in such a manner would not be in compliance with publicly available technical requirements. CTIA argues, however, that there is no need for a carrier to redesign its network to create information for use by a LEA.[35]

19. Numerous parties take issue with the contention of DoJ/FBI that "reasonable availability" is only a technical concept, and others argue that costs should be taken into consideration even for punch list items that are not considered to be call-identifying information. Ameritech Corporation (Ameritech) maintains that Congress used the term "reasonable availability" to include not only technical but also cost and timeliness considerations.[36] PrimeCo Personal Communications, L.P. (PrimeCo) argues that DoJ's/FBI's interpretation of this term would effectively nullify Congress's imposition of a reasonableness requirement and would require the redesign of networks and equipment upgrades without regard to cost considerations.

---

[33] DoJ/FBI Comments, at 21-25.

[34] Nextel Reply Comments, at 6-7.

[35] CTIA Reply Comments, at 28-29.

[36] Ameritech Reply Comments, at 4.

According to PrimeCo, such an interpretation would eviscerate the safe harbor of section 107 by requiring carriers to provide a particular punch list capability notwithstanding the cost criteria set forth in section 107(b).[37] The United States Telephone Association (USTA) agrees, stating that we cannot adopt a punch list item unless it is shown to meet those cost criteria.[38] AirTouch states that the cost of any technical solution is necessarily part of a determination as to whether that solution is reasonably available.[39] AT&T states that section 107(b)(1) provides that if a capability cannot be provided in a cost-effective manner, that capability need not be provided.[40]

20. Several parties who argue that the costs of a particular punch list capability are relevant to a determination of whether that capability is reasonably available to carriers also argue that we must take into account the costs of the core interim standard in our determination of whether a punch list item should be required. CTIA contends that these costs will be in excess of $4 billion for all carriers.[41] On a per switch basis, AT&T states that these costs, even excluding some that are difficult to quantify, approach almost $500,000.[42] The Personal Communications Industry Association (PCIA) maintains that, based on the lowest switch modification costs in the record, the nationwide cost to local exchange carriers (LECs) of implementing the interim standard will be $1.73 billion; and, based on AT&T's per switch estimates, nationwide costs to wireless carriers will be $639 million.[43]

21. Ameritech proposes that if the cost of developing a punch list capability exceeds 5% of the interim standard we should deem that capability to be not reasonably available.[44] Additionally, Ameritech asserts that we must consider the cost of modifying switches placed into service on or before January 1, 1995 in determining capability requirements under section 103 because any such switches that have undergone major modifications or significant upgrades must be retrofitted at carriers' expense.[45] Ameritech expresses concern that, given the FBI's proposed

[37] PrimeCo Reply Comments, at 2.

[38] USTA Reply Comments, at 3.

[39] AirTouch Reply Comments, at 9.

[40] AT&T Reply Comments, at 5.

[41] CTIA Reply Comments, at 12.

[42] *Id.* at 28.

[43] PCIA Reply Comments, at 6-7.

[44] Ameritech Comments, at 3.

[45] 47 U.S.C. § 1008(d).

definition of "major modification or significant upgrade," a substantial portion of the costs of CALEA compliance are designed to become carriers' responsibilities.[46]

22. DoJ/FBI argue that the telecommunications industry has agreed to bear the costs of implementing the interim standard; therefore, the only relevant costs are the additional costs that will be added by the punch list.[47] Additionally, DoJ/FBI assert that the features required for a carrier to meet its CALEA assistance capability obligations will be among many features contained in one or more periodic "releases" deployed on the carrier's switches, and that the costs attributable to CALEA are only those that will be added to the costs of this regular release process.[48] Further, according to DoJ/FBI, it is general industry practice for carriers to be given discounts of as much as 65% from the manufacturers' quoted prices.[49] Moreover, DoJ/FBI assert that even if CTIA's worst-case scenario in industry-wide compliance costs to implement the J-Standard is accepted and all costs are passed on to consumers, the resulting increase in the average ratepayer's monthly bill would be minimal if costs are spread over five years.[50]

23. In response to our request in the *Further NPRM*,[51] we received comments from five manufacturers regarding their anticipated revenues from selling software, and in some cases certain hardware, to wireline, cellular, and broadband PCS carriers to allow those carriers to meet the technical requirements of CALEA.[52] Subsequently, the Commission's Office of Engineering and Technology (OET) issued a *Public Notice* that solicited comment on these aggregated revenue estimates.[53] These estimates, which would represent costs to the carriers, totalled $916 million for the core J-STD-025 and $414 million for the nine punch list items.[54]

---

[46] Ameritech Reply Comments, at 5.

[47] DoJ/FBI Comments, at 17.

[48] DoJ/FBI Reply Comments, at 14.

[49] *Id.* at 16.

[50] *Id.* at 19.

[51] *Further NPRM*, at ¶ 30.

[52] Each manufacturer requested confidential treatment of its individualized revenue data, and such treatment was granted by the Commission's Office of Engineering and Technology (OET). *See Order*, CC Docket No. 97-213, DA 99-412, released March 2, 1999. Accordingly, in light of OET's ruling, the data were released to the public for comment and considered by the Commission only in aggregated form.

[53] *See Public Notice*, CC Docket No. 97-213, DA 99-863, released May 7, 1999.

[54] *See* Appendix B, *infra*.

24. In response to the *Public Notice*, we received a number of comments concerning the aggregated revenue estimates. CTIA contends that its survey of 21 wireless carriers and six wireless switch manufacturers generally confirms these estimates.[55] AirTouch states that the estimates provide a floor that the actual total is sure to exceed, and asserts that the Commission must conclude that the punch list is not cost-effective. AirTouch argues that carriers will incur extensive expenses that will not be paid to telecommunications equipment manufacturers, including in-house engineering and implementation costs and purchases from third-party suppliers.[56]

25. GTE and SBC agree with AirTouch that the manufacturers' revenue estimates significantly understate total costs, and each provides its own CALEA compliance cost estimates. GTE states that many of its switches are not manufactured by the five vendors encompassed by the *Public Notice*, and further states that it has one of the most central office-intensive networks in the country, thereby increasing its CALEA compliance costs. According to GTE, its wireline costs of implementing J-STD-025 are more than $400 million, which compares with the manufacturers' wireline revenue estimate of only $569 million.[57] SBC states its CALEA compliance cost estimates include not only software, but activation fees, engineering and installation fees, gating hardware costs, and the required advancement of generic upgrades. Based on these total costs, SBC estimates its wireline J-STD-025 compliance costs to be $326 million, and its wireless J-STD-025 compliance costs to be $37.2 million. SBC also estimates its wireline CALEA compliance costs, including the costs associated with the punch list, to be $340 million, with punch list costs unavailable for its wireless carriers.[58]

26. DoJ/FBI contend that the manufacturers' revenue estimates have no relevance to the Commission's task under section 107(b) of CALEA.[59] DoJ/FBI further contend that these estimates are overstated because they reflect list prices, and additionally do not take into account the fact that a substantial portion of costs to carriers will be reimbursed because equipment was installed or deployed by January 1, 1995. DoJ/FBI also maintain that the estimates may include revenues that enable carriers to meet CALEA's capacity, rather than capability, requirements; and further, may reflect CALEA solutions being incorporated into all remote switches.[60] DoJ/FBI

[55] CTIA Comments to *Public Notice*, at 3, 7.

[56] AirTouch Comments to *Public Notice*, at 2-4.

[57] GTE Reply Comments to *Public Notice*, at 5-6.

[58] SBC Comments to *Public Notice*, at 1-3.

[59] DoJ/FBI Comments to *Public Notice*, at 1.

[60] *Id.* at 6-8.

note that under section 104(e) of CALEA, eligible capacity costs incurred by a carrier are to be reimbursed by the Government;[61] and argue that for many switching platforms, compliance solutions need to be incorporated only into host and stand-alone switches, and not into remote switches.[62]

27. USTA asserts that there is no evidence that any discounts from list prices are available to reduce costs to carriers, and contends that the DoJ/FBI interpretations of the meaning of the terms "equipment, facilities, or services installed or deployed" by January 1, 1995 and "major modifications" to such equipment, facilities, or services would limit reimbursement to carriers. Additionally, USTA maintains that there has been no indication from DoJ/FBI as to what capacity costs will be eligible for reimbursement.[63]

28. *Discussion.* We reiterate that we find no need to re-examine the entire interim standard;[64] however, in addition to examining the eleven alleged deficiencies, we also will examine any specific issue regarding that standard raised by the proposals in the *Further NPRM*, including the definition of "reasonably available." The interim standard states that call-identifying information is "reasonably available" to a carrier if such information is present at an IAP for call processing purposes.[65] We agree with DoJ/FBI that J-STD-025's definition of "reasonably available" is too narrow because the definition would limit "reasonably available call-identifying information" to call-identifying information used by the IAP switch for call processing. On the other hand, we find DoJ/FBI's proffered definition unnecessarily broad because it would apply to call identifying information located anywhere within a carrier's network, rather than at the IAP location where the information is being captured for the LEA. Consequently, we do not disturb the interim standard's conclusion that call identifying information is reasonably available if it is located at the IAP. We thus find that if call-identifying information is present at a carrier's IAP[66] and can be made available without the carrier being unduly burdened with network modifications, that information is reasonably available to that carrier, even if it is not used by the IAP switch for call processing. Under this definition, call-identifying information that is used by the IAP

[61] 47 U.S.C. § 1003(b).

[62] DoJ/FBI Comments to *Public Notice*, at 8.

[63] USTA Reply Comments to *Public Notice*, at 2.

[64] *See* ¶ 13, *supra.*

[65] *See* ¶ 14 and n.30, *supra*; and *see again* § 4.2.1 of J-STD-025, at 13. The intercept access point is the point in the network where the subscriber's phone line is tapped, usually at the switch.

[66] As mentioned in ¶ 14, *supra*, there may be more than one IAP within a carrier's network.

switch for call processing is reasonably available, as well as other call-identifying information carried on the carrier's network that passes the IAP.

29. We believe that modifying the definition of "reasonably available" to include call identifying information that is present at an IAP, as opposed to restricting such information to that used only for call processing, serves the important objective of not impeding the development of new communications services. In addition to network design considerations, our modification will permit cost and privacy considerations to be considered in determining whether call-identifying information is "reasonably available" to an originating carrier. This modification is consistent with most commenting parties' contention that the term "reasonably available," as set forth in section 103(a)(2) of CALEA, is best interpreted to include cost factors in addition to technical considerations. We believe that this interpretation is consistent with the Act's directive that in taking any action under section 107(b), the Commission must meet the assistance capability requirements of section 103 by cost-effective methods and minimize the cost of CALEA compliance on residential ratepayers, as well protecting the privacy and security of communications not authorized to be intercepted.[67] Accordingly, we will define call-identifying information to be "reasonably available" to an originating carrier if such information "is present at an IAP and can be made available without the carrier being unduly burdened with network modifications."

30. We have reviewed the cost/revenue data submitted in this proceeding. While there are a wide variety of cost estimates, we find the five manufacturers' aggregate revenue estimates of $916 million for the core J-STD-025 and $414 million for the nine punch list items to be a reasonable guide of the costs to wireline, cellular, and broadband PCS carriers for CALEA compliance. Commenters have noted reasons for believing that the manufacturers' revenue estimates may either understate or overstate costs to carriers. On balance, we find that while these estimates indicate that costs to carriers will be significant, and do not represent all carrier costs of implementing CALEA,[68] the additional punch list costs are not so exorbitant as to require us to reject the punch list automatically without considering each item on an individual basis in relation to CALEA's other statutory factors. We find particularly instructive the cost of the punch list relative to the cost of the core J-STD-025 because the latter represents the bulk of costs to carriers, and carriers -- through their participation in TIA Subcommittee TR45.2 -- have agreed to provide the core capabilities of J-STD-025. Accordingly, we will evaluate each punch list item individually, including the anticipated cost of each item, as discussed below.

[67] 47 U.S.C. § 1006(b).

[68] As OET noted in its *Public Notice*, the revenue estimates are for only five manufacturers, and do not represent all CALEA-related software and equipment revenues anticipated by these manufacturers. *See Public Notice*, at ¶ 4. Nevertheless, relative to other cost/revenue estimates submitted in this proceeding, we find the manufacturers' estimates to be the most detailed and reliable.

31. We decline to adopt Ameritech's proposals relating to costs. Its proposal for the Commission to automatically reject any punch list capability whose costs exceed 5% of the interim standard would necessarily be arbitrary and contrary to our directives under CALEA. Additionally, while we recognize that some switches placed into service on or before January 1, 1995 may have to be retrofitted at carriers' expense, the commenting parties have not submitted information sufficient for us to quantify the impact of this factor.

3. Retrofitting Equipment under Interim Standard

32. Bell Atlantic Mobile, Inc. (BAM) raises another concern about the interim standard. BAM argues that, in cases in which a carrier deployed equipment after January 1, 1995, we should commence a proceeding under section 109(b) of CALEA to decide whether the carrier should be required to bear the costs of retrofitting that equipment to comply with the interim standard.[69] BAM contends that we are empowered with broad authority to alleviate the adverse public policy implications for competition and consumers of requiring carriers to pay for retrofitting equipment.[70]

33. *Discussion.* We observe that BAM's request that the Commission undertake a rulemaking proceeding under section 109(b) to decide generally whether telecommunications carriers should be required to bear the costs of retrofitting equipment installed after January 1, 1995 is contrary to the plain language of the Act. Section 109(b) requires us to determine upon receipt of a petition whether compliance by an individual carrier with the assistance capability requirements of section 103 is reasonably achievable with respect to any equipment, facility, or service installed or deployed after January 1, 1995.[71] If we receive a petition and determine that compliance by an individual carrier is not reasonably achievable, the Act provides that the Attorney General may agree to pay for any such equipment, facility or service.[72] If the Attorney

---

[69] Carriers do not have to pay to retrofit equipment installed on or before January 1, 1995 if it has not been significantly upgraded or otherwise modified since that time. Section 109 of CALEA provides that "[t]he Attorney General may, subject to the availability of appropriations, agree to pay telecommunications carriers for all reasonable costs directly associated with the modifications performed by carriers in connection with equipment, facilities, and services installed or deployed on or before January 1, 1995, to establish the capabilities necessary to comply with section 103." 47 U.S.C. § 1008(a). If the Attorney General does not agree to pay all reasonable costs directly related to such modifications, the "equipment, facility, or service [deployed on or before January 1, 1995] shall be considered to be in compliance with the assistance capability requirements of section 103 until the equipment, facility, or service is replaced or significantly upgraded or otherwise undergoes major modification." 47 U.S.C. § 1008(d).

[70] BAM Comments, at 15-16.

[71] 47 U.S.C. § 1008(b)(1).

[72] 47 U.S.C. § 1008(b)(2).

General does not agree to pay, that carrier shall be deemed to be in compliance with the assistance capability requirements of section 103.[73] Accordingly, we decline to adopt BAM's proposal since it is contrary to the plain language of the Act.[74]

4. Compliance Date for Interim Standard

34. AirTouch Communications, Inc. (AirTouch); BellSouth Corporation, Inc., BellSouth Telecommunications, Inc., BellSouth Cellular Corp., BellSouth Personal Communications, Inc., and BellSouth Wireless Data, L,P. (BellSouth); and SBC Communications, Inc. (SBC) question whether the current June 30, 2000 deadline for implementation of the core requirements of the interim standard is achievable. AirTouch states that we should acknowledge in this *Third R&O* that additional extensions may be necessary;[75] BellSouth states that only one of its vendors has promised to meet the current deadline;[76] and SBC states that the delivery schedule contemplated by its vendors will not allow for the extensive testing required to ensure that its deployment is in compliance with the interim standard, nor does this schedule allow a sufficient period for deployment across SBC's entire network.[77]

35. *Discussion.* We see no reason at this time to extend, on an industry wide basis, the June 30, 2000 deadline for compliance with CALEA's section 103 capability requirements that are covered by the interim standard. We observe that the deadline specified in the Act was October 25, 1998;[78] thus, we have already extended the original deadline by more than 20 months. In our *Extension Order,* we stated:

> [W]e will require carriers to have installed CALEA-compliant equipment and facilities based on the core J-STD-025 standard by June 30, 2000. This is a firm deadline. If this

---

[73] *Id.*

[74] We note that in a companion item adopted simultaneously with this order, we provide guidance regarding the factors that we will consider in making determinations under section 109(b) as to whether compliance with CALEA's assistance capability requirements is reasonably achievable for particular carriers, and the showings we expect entities filing petitions under section 109(b) to make. *See Second Report and Order*, CC Docket No. 97-213, FCC 99-229, adopted August 26, 1999.

[75] AirTouch Comments, at 31.

[76] BellSouth Comments, at i.

[77] SBC Comments, at 18-19.

[78] Section 111(b) of CALEA, 47 U.S.C. § 1001(b), specified a compliance deadline four years after the Act's enactment. The Act was enacted on October 25, 1994; accordingly, the original compliance deadline was October 25, 1998.

standard is ultimately modified and new capabilities or features are added to the core standard in the section 107(b) rulemaking, we will consider establishing a separate deadline for upgrading carrier equipment and facilities to comply with those capabilities or features in that proceeding pursuant to our authority under section 107(b)(5). This approach provides certainty to the telecommunications industry in developing and installing CALEA-compliant solutions, and recognizes the interests of law enforcement in providing effective public safety. It also seeks to allow carriers to implement a CALEA-compliant solution sooner, rather than later, while providing the flexibility to design modifications to the core J-STD-025 standard that can be installed in carrier equipment and facilities in subsequent upgrades, if any such modifications are adopted in the section 107(b) rulemaking proceeding.[79]

36. Therefore, carriers and manufacturers have been on notice since the September 1998 *Extension Order* that we considered June 30, 2000 a "firm" deadline for the section 103 capability requirements covered by the J-STD-025.[80] Additionally, as discussed in paragraph 129, *infra*, we find the record justifies the establishment of a separate later deadline for the additional capabilities that we are herein mandating for wireline, cellular, and broadband PCS carriers. We also note that DoJ/FBI is currently negotiating with carriers regarding areas where wiretaps are infrequent, and these carriers may be permitted to postpone CALEA compliance in those areas.[81] Accordingly, we understand that DoJ/FBI and/or the affected carriers may seek an extension under section 107(c) of CALEA of the June 30, 2000 deadline in conformance with such agreements.[82] We therefore will await receipt of such requests before deciding on a new deadline for the affected carriers. We expect that along with such requests, DoJ/FBI will submit a list of the affected carriers and the terms of such extensions so that we may place such information on Public Notice for comment.

---

[79] *Memorandum Opinion and Order*, CC Docket No. 97-213, FCC 98-223, released September 11, 1998, at ¶ 46 (footnote omitted).

[80] The *Extension Order* stated that the "core" of J-STD-025 excludes both the provision of location information and packet-mode communications. *Id.* at n.139. However, in the *Further NPRM* we proposed to modify that conclusion to include a location information feature as part of the core of J-STD-025. *See Further NPRM*, at ¶ 46. As discussed in ¶ 46, *infra*, we are herein adopting that proposal and are requiring that a location information feature be deployed by carriers by the June 30, 2000 CALEA compliance deadline, unless carriers have obtained an extension. With respect to packet-mode communications, as discussed in ¶ 55, *infra*, we are herein requiring that a packet-mode feature be deployed by September 30, 2001.

[81] *See* letter of June 30, 1999, from Stephen R. Colgate, Assistant Attorney General for Administration, to William E. Kennard, Chairman, Federal Communications Commission.

[82] We recognize that CALEA also permits carriers to file petitions under section 109(b) of CALEA stating that compliance with the assistance capability requirements of section 103 is not reasonably achievable with respect to any equipment, facilities, or equipment deployed after January 1, 1995.

B. Particular Capabilities of J-STD-025 Opposed by CDT, EFF, EPIC, and ACLU

1. Location Information

37. *Background.* J-STD-025 includes a "location" parameter that would identify the location of a subject's "mobile terminal" whenever this information is reasonably available at the intercept access point and its delivery to law enforcement is legally authorized. Location information would be available to the LEA irrespective of whether a call content channel or a call data channel was employed.[83]

38. The *Further NPRM* tentatively concluded that location information falls under the definition of call-identifying information set forth in section 102(2) of CALEA because location information identifies the origin or destination of a communication.[84] Therefore, the *Further NPRM* proposed that where location information is reasonably available to a carrier, provision of that information to LEAs is necessary to meet the mandates of section 103. The *Further NPRM* also proposed that location information necessary to meet section 103 would include only the subject's cell site location at the beginning and termination of a call. Finally, the *Further NPRM* tentatively concluded that for a LEA to obtain location information that cannot be determined from the telephone number, the LEA must have an authorization different from the minimal authorization necessary for use of pen registers and trap and trace devices.[85]

39. *Comments.* CDT states that our tentative decision to require carriers to design a location capability into wireless phones cannot be supported by the plain words of CALEA and, further, directly contradicts the Act's legislative history, which states that location information is not a CALEA mandate.[86] CDT contends that the words "origin" and "destination" have obvious meanings apart from location, and that interpreting those terms to also mean cell site location violates a fundamental rule of statutory interpretation -- that each word in a statute should be given a single and unique meaning. Also, CDT contends that the location of wireless phones is more personally revealing than the location of wireline phones because when a call is made on a wireless phone it almost always is made by the individual subscriber.[87]

---

[83] J-STD-025 at § 6.4.6, and at §§ 5.4.1-5.4.8, Tables 1, 5, 6, and 8.

[84] 47 U.S.C. § 1001(2).

[85] *Further NPRM*, at ¶¶ 52-57.

[86] CDT Reply Comments, at iii.

[87] CDT Comments, at 5-12.

40. EPIC, EFF, and ACLU generally agree with CDT, arguing that CALEA contains no provisions expressly including location tracking data within the definition of call-identifying information. EPIC, EFF, and ACLU also contend that the interim standard is internally inconsistent because it proposes to require carriers to provide location tracking data at the beginning and end of calls as part of their duty to provide information regarding the "origin" and "destination" of particular communications, but the definition of those terms in the interim standard does not pertain to physical location.[88]

41. US West states that the location information capability in the interim standard is not call-identifying information under section 103(a). US West argues that CALEA's definition of call-identifying information requires carriers to provide LEAs with telephone numbers, not other characteristics of calls. US West maintains that while a LEA generally is able to derive a target's physical location from a telephone number for most wireline calls, that ability is incidental and should not be read as an underlying mandate of CALEA.[89]

42. DoJ/FBI argue that location information is call-identifying and state that, irrespective of whether we modify the definition of "reasonable availability" as they propose, there is no need for us to interpret or construe this term differently in connection with location information than in connection with the other kinds of call-identifying information at issue in this proceeding.[90] DoJ/FBI state that they agree that the interim standard requires only that cell site location at the beginning and end of a call be provided, and maintain that CALEA embodies a compromise regarding location information: When a LEA is proceeding "solely pursuant to the authority for pen registers and trap and trace devices," carriers are not to treat location information as call-identifying information, but when a LEA has been duly authorized to acquire location information under other electronic surveillance statutes, location information remains part of call-identifying information. DoJ/FBI contend that the interim standard is consistent with this intent, while CDT's position is not. DoJ/FBI state that it is not the case, as CDT suggests, that the Commission's reading of "origin" and "destination" gives those terms different meanings for wireless and wireline communications. DoJ/FBI contend that those terms encompass location both in the wireless and wireline settings, but that in the case of wireline communications the fixed location of the subscriber's terminal means that the telephone number of the terminal identifies the location of the call, and so no separate location information is required.[91]

---

[88] EPIC, EFF, and ACLU Reply Comments, at 10-11. Page 5 of J-STD-025 states that "origin is the number of the party initiating a call (e.g., calling party)" and "destination is the number of the party to which a call is being made (e.g., called party)."

[89] US West Comments, at 24.

[90] DoJ/FBI Comments, at 74-76.

[91] DoJ/FBI Reply Comments, at 66-68.

43. The New York City Police Department (NYPD) argues that any location information that is used and/or is available within a carrier's network for the purpose of providing overall service and/or processing of individual calls should be considered by us to be reasonably available to the carrier in the case of location of wireless devices. However, NYPD expresses concern about our proposal to adopt cell site location rather than a more precise location for the subject's mobile terminal. NYPD contends that such a broad definition could limit the scope of existing electronic surveillance authority. For example, NYPD states that in criminal cases where triangulation techniques that allow location to be determined with exactitude have been authorized by a court, carriers might be reluctant to assist a LEA to determine a more precise location than a cell site.[92]

44. *Discussion.* We find that a subject's cell site location at the beginning and end of a call is call-identifying information under CALEA. The Act states that call-identifying information is "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier."[93] We find, contrary to the position of CDT and EPIC/EFF/ACLU, that a subject's cell site location at the beginning and end of a call identifies the "origin" or "destination" of a communication and thus is covered by CALEA. With respect to CALEA's express statement that "with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127 of title 18, United States Code), . . . call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number),"[94] we agree with DoJ/FBI that this provision does not exclude location information from the category of "call-identifying information," but simply imposes upon law enforcement an authorization requirement different from that minimally necessary for use of pen registers and trap and trace devices.[95]

---

[92] NYPD Comments, at 7-8.

[93] 47 U.S.C. § 1001(2).

[94] 47 U.S.C. § 1002(a)(2)(B).

[95] As we stated in the *Further NPRM*, we believe that interpreting this provision to exclude location information from the technical requirements for CALEA would render the provision "mere surplusage" and would thus conflict with the usual rules of statutory construction. *See Dunn v. CFTC*, 519 U.S. 465 (1997), 117 S.Ct. 913, 917 (1997) ("legislative enactments should not be construed to render their provisions mere surplusage"); *Illinois Public Telecommunications Ass'n v. FCC*, 117 F.3d 555, 562 (D.C.Cir. 1997) (construing section 226(e)(2) of Communications Act in manner to avoid "mere surplusage"); *Deployment of Wireline Services Offering Advanced Telecommunications Capability*, CC Docket No. 98-147, Memorandum Opinion and Order and Notice of Proposed Rulemaking, FCC 98-188, released August 7, 1998, at ¶ 71 ("when . . . 'charged with understanding the relationship between two different provisions within the same statute, we must analyze the language of each to make sense of the whole'").

45. Additionally, we find that location information is reasonably available to cellular and broadband PCS carriers. We observe that this capability was developed by industry and is included in the interim standard. Further, as we observed in the *Further NPRM*, in the wireline environment LEAs have generally been able to obtain location information routinely from the telephone number because the telephone number usually corresponds with location. With the telephone number, location information is available from a LEA's own 911/Enhanced 911 (E911) database or from the telephone company's electronic records, such as the Loop Maintenance Operating System (LMOS).[96] We also note that the equivalent location information in the wireless (cellular or broadband PCS) environment appears to be the location of the cell sites to which the mobile terminal or handset is connected at the beginning and at the termination of the call. Provision of this particular location information does not appear to expand or diminish law enforcement's surveillance authority under prior law applicable to the wireline environment.

46. We will not, however, mandate a location tracking capability in this proceeding. While NYPD believes that a capability that identifies location more precisely would be useful to LEAs, we are concerned that such a capability poses difficulties that could undermine individual privacy. We believe that a more generalized capability that will identify only the location of a cell site, and only at the beginning and termination of the call, will give LEAs adequate information. We note, however, that our decision herein does not preclude LEAs from requesting legal authority to acquire more specific location information in particular circumstances. Accordingly, as has been agreed to by both DoJ/FBI and the telecommunications industry, we mandate a location capability that will identify cell site location at the beginning and termination of a call. As proposed in the *Further NPRM*, we require that this capability be deployed by carriers by the June 30, 2000 CALEA compliance deadline, unless carriers have obtained an extension.

2. Packet-Mode

47. *Background.* J-STD-025 provides for LEA access to call-identifying information and the interception of wire and electronic telecommunications, regardless of whether the telecommunications are carried in circuit-mode or in packet-mode.[97] It further states that the "call-identifying information associated with the circuit-mode content surveillance is provided on

[96] *See* Transmission Systems for Communications, AT&T Bell Laboratories (5th ed. 1982).

[97] *See* J-STD-025, at §§ 3 and 4.5. Section 3 of J-STD-025 defines circuit-mode as "a communication using bi-directional paths switched or connected when the communication is established. The entire communication uses the same path." Section 3 defines packet-mode as "a communication where individual packets or virtual circuits of a communication within a physical circuit are switched or routed by the accessing telecommunication system. Each packet may take a different route through the intervening network(s)."

the [call data channel]," but does not specifically address whether call-identifying information, if any, associated with packet-mode surveillance must be provided over a call data channel.[98]

48. The *Further NPRM* noted that packet data and packet-switching technology are potentially usable for both information services and telecommunications services, but that such technology is subject to CALEA requirements only to the extent it is used to provide telecommunications services, and not for information services. The *Further NPRM* also noted that privacy concerns could be implicated if carriers were to give to LEAs packets containing both call-identifying and call content information when only the former was authorized. The *Further NPRM* tentatively concluded that the record is not sufficiently developed to support any particular technical requirements for packet-mode communications, and therefore did not propose technical requirements for such communications. However, the *Further NPRM* sought comment on a wide range of issues to develop a sufficient record.[99]

49. *Comments.* EFF, EPIC, and ACLU state that our cautious approach regarding packet-mode communications is correct, and that it is critical that we adequately protect the privacy of communications carried on packet-mode systems. They state that the interim standard's requirement to deliver the entire packet data stream associated with a given communication violates the privacy provisions of section 103. Therefore, according to EFF, EPIC, and ACLU, until carriers are able to protect the privacy of communications carried over packet-mode systems, we should refrain from adopting capability requirements for such systems.[100]

50. CDT states that carriers using packet technologies have an obligation under CALEA to protect privacy by distinguishing between call content and call-identifying information, so that a LEA does not intercept the former when it has only the narrower authority for the latter. CDT contends that DoJ/FBI acknowledge that protecting privacy by distinguishing between call content and call-identifying information is technically trivial, but states that DoJ/FBI believe there is no obligation on carriers to protect privacy. CDT states that we should not wait until packet technologies are more fully deployed to clarify that carriers have an obligation to protect individual privacy.[101]

---

[98] *Id.*

[99] *Further NPRM,* at ¶¶ 63-66.

[100] EPIC/EFF/ACLU Reply Comments, at 8-10.

[101] CDT Reply Comments, at ii-iii.

51. AT&T supports our tentative conclusion that packet-mode technologies may require differing CALEA solutions. AT&T states that it believes that if we defer setting packet-mode communications standards in this proceeding, industry associations will take up the issue on their own.[102]

52. TIA states that the telecommunications network is rapidly evolving toward a packet-based architecture. TIA cautions that the Commission not stifle the continued development of packet-mode technologies by imposing a solution that could require the redesign (or even abandonment) of certain technologies. TIA recommends that we consider establishing a separate packet-mode standard-setting effort within it.[103]

53. US West argues that risks to advanced services and the Internet support the deferral of any CALEA requirements on packet networks, at least until CALEA can be implemented without inhibiting the development of advanced telecommunications services. It further states that because many packet-mode communications will avoid the circuit-switched network altogether, carriers and manufacturers will have to develop and install CALEA solutions for different network elements from those used in circuit-switched networks. Additionally, US West asserts that separating the header from content in packet-mode communications is not feasible because packet data is delivered in a layered stack structure, and carriers have neither the ability nor any business reason to monitor packet data streams and then decipher the various protocols.[104]

54. DoJ/FBI argue that the interim standard's treatment of packet-mode communications in pen register cases does not conflict with anything in CALEA, and hence that standard is not deficient in this regard. DoJ/FBI state that, as a technical matter, it is perfectly feasible for a LEA to employ equipment that distinguishes between a packet's header and its communications payload and makes only the relevant header information available for recording or decoding. DoJ/FBI further state that the statutory distinction between telecommunications carriers and providers of information services does not correspond to any distinction between packet-mode and circuit-mode communications; therefore, the use of packet-mode protocols does not turn the transmission of a wire or electronic communication by a telecommunications carrier into the provision of information services.[105]

---

[102] AT&T Comments, at 25.

[103] TIA Comments, at ii, 47.

[104] US West Comments, at i-ii and 27-28.

[105] DoJ/FBI Comments, at 79-82.

55. *Discussion.* We find that the approach taken with regard to packet-mode communications in J-STD-025 raises significant technical and privacy concerns. Under this standard, LEAs would be provided with both call-identifying information and call content even in cases where a LEA is authorized only to receive call-identifying information (*i.e.*, under a pen register). We are aware that packet-mode technology is rapidly changing, and that different technologies may require differing CALEA solutions for separating call-identifying information from call content.[106] We also recognize that we must avoid implementing CALEA requirements that could impede the development of new technologies. We do not believe that the record sufficiently addresses packet technologies and the problems that they may present for CALEA purposes. For example, some packet technologies (e.g., frame relay, ATM, X.25) are connection oriented--i.e., there are call set-up and take-down processes, similar to those used in circuit switched voice networks, whereby addressing information is made available to the carrier separate from and before call content is transmitted. Other packet technologies (e.g., internet protocol based solutions) would not be processed this way. We believe that further efforts can be made to find ways to better protect privacy by providing law enforcement only with the information to which it is lawfully entitled. We note that TIA recommends further study of this matter. Accordingly, we invite TIA to study CALEA solutions for packet-mode technology and report to the Commission in one year on steps that can be taken, including particular amendments to J-STD-025, that will better address privacy concerns. In the interim, we find that packet-mode communications, including call-identifying information and call content, may be delivered to law enforcement under the interim standard.[107] Further, we are herein requiring that packet-mode communications be delivered to LEAs under that standard no later than September 30, 2001.[108] That date is 15 months after the June 30, 2000 CALEA compliance deadline, and will afford manufacturers that have not yet developed a packet-mode capability the time needed to do so.

---

[106] For example, J-STD-025 itself states that a packet data IAP provides access to the following eight packet-mode services: Integrated Services Digital Network (ISDN) user-to-user signaling; ISDN D-channel X.25 packet services; Short Message Services (SMS) for cellular and broadband PCS (*e.g.*, NAMPS, *TIA/EIA-41*, PCS1900, or GSM-based technologies); wireless packet-mode data services (*e.g.*, Cellular Digital Packet Data (CDPD), Code Division Multiple Access (CDMA), Time Division Multiple Access (TDMA), PCS1900, or GSM-based packet-mode services); X.25 services; TCP/IP services; paging (one-way or two-way); and packet-mode services using traffic channels. J-STD-025 at § 4.5.2. In addition, we note that there may be other packet technologies warranting discussion. This appears especially so, given that many carriers now provide so-called fast packet services such as frame relay and Asynchronous Transfer Mode (ATM).

[107] We recognize that call identifying information for packet technologies also may be acquired from the carrier's records.

[108] In the *Further NPRM*, we stated that we would set a separate deadline for compliance with the additional technical requirements that we determine CALEA mandates. *See Further NPRM*, at ¶ 133. We note that we are also adopting a September 30, 2001 compliance date for the six punch list items that we are herein mandating. *See* ¶ 129, *infra*.

56. We recognize that the solution we have crafted above is not perfect because a LEA may receive both call identifying information and call content under a pen register. We note, however, that independent legal barriers exist which will protect, to a certain extent, the privacy rights of individuals until a permanent solution is developed. In particular, under this interim arrangement the LEA will be legally prohibited from using any content information in a court proceeding if it has only a pen register or trap and trace authorization.[109] We find, therefore, that in weighing the factors identified under section 107(b) of CALEA--that is, in particular, (1) to meet the assistance capability requirements of section 103 by cost effective methods, (2) to protect the privacy and security of communications not authorized to be intercepted, and (3) to encourage the provision of new technologies and services to the public --we believe that the above solution provides the most suitable temporary remedy available at this time. We emphasize, however, that we intend this solution to be only an interim one. We recognize that, in view of the growing importance of packet-mode communications, a timely permanent solution is essential. Accordingly, we expect that TIA will deliver a report to us no later than September 30, 2000 that will detail a permanent solution, keeping in mind the objectives underlying CALEA which are described in paragraph 2, *supra*.

C. DoJ/FBI Punch List

57. Section 103(a)(1) of CALEA authorizes telecommunications carriers to provide to LEAs call content information, pursuant to a court order or other lawful authorization; and section 103(a)(2) of CALEA authorizes telecommunications carriers to provide to LEAs call-identifying information, pursuant to a court order or other lawful authorization.[110] Call-identifying information, however, must be provided only if it is reasonably available to the carrier.[111] The *Further NPRM* tentatively concluded that the provision by carriers to LEAs of the content of subject-initiated conference calls is authorized by section 103(a)(1); and that party hold, join, drop on conference calls, subject-initiated dialing and signaling information, timing information, and dialed digit extraction constitute call-identifying information under section 102(2) of CALEA and therefore must be provided, where reasonably available, under section 103(a)(2).[112]

1. Content of subject-initiated conference calls

[109] *See* 18 U.S.C. §§ 2515 and 2518.

[110] 47 U.S.C. § 1002(a)(1)-(2).

[111] 47 U.S.C. § 1002(a)(2).

[112] *Further NPRM*, at ¶¶ 77-79, 85-87, 91-94, 104-105, and 128.

58. *Background.* This capability would permit the LEA to monitor the content of conversations connected via a conference call set up by the facilities under surveillance. Surveillance of all portions of a conference call would continue, even if any party to the call utilized services such as hold, call waiting, or three-way calling. For example, if anyone involved in a conference call were placed on hold, all remaining conversations would continue to be available to the LEA for monitoring. The ability to monitor would continue even after the subject drops off the conference call.

59. The *Further NPRM* tentatively concluded that the provision to LEAs of the content of subject-initiated conference calls is a technical requirement that meets the assistance capability requirements of section 103(a) of CALEA. The *Further NPRM* also sought comment as to how the Commission should define or interpret section 103's use of the phrase "equipment, facilities, or services" in the context of subscriber-initiated conference calls.[113] The five manufacturers' aggregate revenue estimate for this capability is $37 million.[114]

60. *Comments.* TIA states that the interim standard already provides LEAs access to the content of most conference calls. TIA contends that access is not provided in only a few situations in which the subject's terminal equipment is not connected to the call. TIA further contends that while providing this capability to LEAs is technically feasible, it would require a large redeployment effort by most manufacturers -- particularly with respect to provisioning a separate call content channel to monitor the conversations of any parties on hold.[115]

61. Bell Atlantic argues that providing the conference calling feature as proposed would give LEAs an expanded capability. Bell Atlantic states that while multi-party calling services and conference calling have been available for many years, LEAs have not had the ability to monitor all parties to a multiparty conference call after the subject of the surveillance has left the call or has put the call on hold.[116] EPIC, EFF, and ACLU agree that our proposal would permit expanded access to conversations of participants in subject-initiated conference calls, and they contend that this expansion would be inconsistent with statutory and constitutional limitations because it would expand the facilities doctrine[117] of Title III of the Omnibus Crime

[113] *Id.* at ¶¶ 77-79.

[114] *See Public Notice*, at 4.

[115] TIA Comments, at 27-28.

[116] Bell Atlantic Comments, at 4.

[117] The parties argue that courts have traditionally considered "facilities" to be a subscriber's terminal equipment or, with conference bridges, the connection between the subscriber's terminal equipment and the subscriber side port of the carrier's switch. EPIC, EFF, and ACLU Comments, at 20-21.

Control and Safe Streets Act of 1968, as modified by the Electronic Communications Privacy Act of 1986.[118] EPIC, EFF, and ACLU state that a LEA with authority to monitor only the subject's facilities should not be permitted to trace conversations on network resources once the subscriber disconnects.[119]

62. AT&T states that not all conference calls are subscriber-based. It maintains that on-demand services such as "Meet Me" conference calling, in which the carrier or a third party provider makes a conference bridge available to anyone, are not covered by CALEA because there is no subscriber.[120] Ameritech agrees, stating that conference bridging services must be excluded because they are not "equipment, facilities, or services of a subscriber." Ameritech contends that such services do not permit carriers to know when conference calls will occur and which telecommunications providers will be used to establish the calls.[121]

63. DoJ/FBI contend that the proposed conference calling capability is consistent with CALEA. They maintain that when a subscriber's service supports the ability of other participants in a conference call to continue to speak to one another when the subscriber places them on hold or hangs up, the conversations of these other participants constitute "communications" to or from the subscriber's "equipment, facilities, or services," and therefore come within the scope of section 103(a)(1). DoJ/FBI also assert that call hold is similar to call forwarding, which the legislative history of the Act makes clear was one of the principal features that Congress intended to reach when it enacted CALEA. DoJ/FBI state that the facilities of callers who have been placed on hold are supported by the subscriber's conference calling service even if the communication is no longer routed through the subscriber's switch to his terminal equipment.[122] DoJ/FBI further argue that commenters' arguments that meet-me conference services are outside the scope of a carrier's obligations under section 103 is repudiated by the interim standard. DoJ/FBI state that a party that contracts for meet-me conference service is no less a subscriber than a party that arranges for conventional conference calling service. Finally, DoJ/FBI contend that in no case would a LEA need to use more than two call content channels to monitor a

[118] Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 212 (1968), and Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (together codified as amended in 18 U.S.C. §§ 2510-2522 and in other sections of 18 U.S.C.). These statutory provisions delineate the scope and limitations of federal wiretap surveillance authority.

[119] EPIC, EFF, and ACLU Comments, at 20-21.

[120] AT&T Comments, at 7-8.

[121] Ameritech Comments, at 6.

[122] DoJ/FBI Reply Comments, at 32, 39.

conference call because DoJ/FBI are not seeking separated delivery of each leg of a held call on a different call content channel.[123]

64. *Discussion.* We find that, under certain circumstances discussed below, the provision of the content of subject-initiated conference calls is a technical requirement that meets the assistance capability requirements of section 103.[124] Under these circumstances, with appropriate lawful authorization, the LEA is entitled to "intercept, to the exclusion of any other communications, all wire and electronic communications carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber."[125]

65. As we stated in the *Further NPRM,* we recognize that different carriers provide conference calling features in various ways and that not all carriers' system architectures are the same.[126] Conference calling features include various types of multi-party calls, such as three-way calling where a bridge is established in the subscriber's serving switch, as well as "meet me" or conference bridge services where a bridge is established at a remote switch of another carrier. Some of these services are available as a standard subscriber option from a customer's presubscribed carrier, while others are available on a demand basis from multiple carriers. Some systems are designed, for example, to allow a conference call that is initiated by the subject to continue among other parties on the call even after the subject drops off the call, either by putting the call on hold or terminating the connection; other systems do not offer this feature. When a system is designed to allow the conference call to continue, we conclude that carriers must provide the content of the call under the following circumstances.

66. Clearly, a LEA, pursuant to a court order or other lawful authorization, is entitled to the content of the conference call when the subject's facilities initiate the call and are being used to participate in the call. In this case, an open circuit is maintained between the subject's equipment, facilities and services and the other parties on the call. When the subject puts the conference call on hold, the subject's circuit to the conference call is maintained within the carrier's network (usually at the subscriber's serving switch), thus allowing the subject to rejoin easily the call without having to reinitiate the circuit. In this case, we find that the communication continues to or from the equipment, facility or service of the subscriber, and thus the carrier also must provide the content of the communication among the other parties to the conference call. In both cases, however, we conclude that the carrier does not have to provide access to the

[123] DoJ/FBI Reply Comments, at 32-35.

[124] 47 U.S.C. § 1006(b).

[125] 47 U.S.C. § 1002(a)(1).

[126] *Further NPRM,* at para. 78.

content of the communication between a participant of the conference call other than the subject and any person with whom that participant speaks on an alternative line; e.g., when A, the subject, is on a conference call with B and C, we conclude that C's conversations with D on call waiting do not have to be provided by the carrier. We also conclude that the anticipated costs to carriers of adding the conference call capability in these cases is not so exorbitant as to require automatic exclusion of the capability. In percentage terms, based on the manufacturers' aggregate revenue estimates, these costs would be 4% of the core interim standard and 9% of the total punch list.[127]

67. We reach a different conclusion when the subject terminates his circuit connection to the conference call. In this case, the communication between other participants no longer is to or from the subscriber's equipment, facilities, and services, and may no longer even be "carried by the carrier within a service area" to or from the subscriber of the carrier, pursuant to section 103(a) and (d).[128] This is especially true with conference bridges located in remote switches of other carriers. We conclude that it is not reasonable to require the carrier to provide at its IAP the communications of other parties continuing on the conference call after the subject terminates his circuit connection to the call because to do so would not be a cost-effective method of implementing the conference call intercept and may not protect the privacy and security of communications not authorized to be intercepted, pursuant to section 107(b).[129] We recognize, as DoJ/FBI acknowledge, that if the subject arranges for a "meet me" conference bridge, the LEA will need a Title III order to cover the communication of the conference bridge.[130] Under

[127] *See* Appendix B, *infra.*

[128] Sections 103 (a)(1) and (d) of CALEA, 47 U.S.C. §§ 1002(a)(1) and (d). Section 103(a)(1) requires a carrier to "ensure that its equipment, facilities, or services ... are capable of ... expeditiously isolating and enabling [lawful interception of] all wire and electronic *communications carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber of such carrier* ..." (italics added). Section 103(d) requires that when a commercial mobile service carrier conducting a lawful interception of wire and electronic communications loses "*access* to the content of such communications or call-identifying information *within the service area* ..., information is made available to the government ... *identifying the provider of a wire or electronic communication service that has acquired access to the communications*'" (italics added).

[129] We recognize that some multi-party calls may be bridged within the subscriber's serving switch, and thus may continue to be within the service area, pursuant to section 103 (a) and (d). Nonetheless, we will not require a carrier to provide the communications of other parties continuing on the call after the subject terminates his connection because to do so may not protect the privacy and security of communications not authorized to be intercepted.

[130] DoJ/FBI Reply Comments, at n.9 (For Title III purposes, a meet-me conference bridge ordinarily will constitute a separate "facility" from the local switch associated with the subscriber's own directory number, and law enforcement therefore will be responsible for obtaining a new Title III order that covers the conference bridge.) Consequently, we do not reach the argument raised by EPIC, EFF and ACLU that implementing the conference call capability as requested by DoJ/FBI would expand Title III's facilities doctrine.

those circumstances, the carrier that provides the conference bridge should provide an IAP to the LEA.[131]

2. Party hold, join, drop on conference calls

68. *Background.* This capability also involves features designed to aid a LEA in the interception of conference calls. This capability would permit the LEA to receive from the telecommunications carrier messages identifying the parties to a conversation at all times. The party hold message would be provided whenever one or more parties are placed on hold. The party join message would report the addition of a party to an active call or the reactivation of a held call. The party drop message would report when any party to a call is released or disconnects and the call continues with two or more other parties.

69. The *Further NPRM* tentatively concluded that this capability constitutes call-identifying information and therefore must be provided by the carrier to the LEA where reasonably available. The *Further NPRM* noted, however, that LEA access to party hold, join, and drop information would be required only in cases where a carrier's facilities, equipment, or services are involved in providing the service; *i.e.*, where a network signal is generated. To the extent that customer premises equipment (CPE) is used to provide this service, the *Further NPRM* tentatively concluded that party hold, join, and drop information could not be made reasonably available to the LEA because no network signal would be generated.[132] The five manufacturers' aggregate revenue estimate for this capability is $64 million.[133]

70. *Comments.* AT&T states that currently carriers do not generate party join and drop messages, and argues that party hold messages are more appropriately classified as subject-initiated signaling. AT&T contends that whether a party joins or drops from a call has no bearing on the continuity of a call or the communications that may be made during the call, and that a call leg does not constitute either a call or a communication. Finally, AT&T argues that if we sustain our tentative conclusion with respect to this capability, we should simply require that industry provide for dynamic reporting of participant changes in a subscriber-initiated conference call because industry may have more efficient or effective ways than party messages to report joins and drops from the call.[134]

---

[131] In some cases, the subject's carrier and the conference bridge carrier may be the same and, indeed, the bridge may be located in the subscriber's serving switch. Thus, in some cases the carrier and the LEA may agree to locate one IAP at a point capable of capturing all communications covered by Title III authority.

[132] *Further NPRM*, at ¶¶ 85-87.

[133] *See Public Notice*, at 4.

[134] AT&T Comments, at 8-10.

71. Bell Atlantic argues that if a carrier were to provide information that a party has been added to or disconnected from a call or has been put on hold, that would be a significant enhancement to existing or previous wiretapping capabilities, and would be beyond the scope of section 103(a)(5). Bell Atlantic also argues that the words "the origin, direction, destination, or termination" in section 102(2) have physical rather than temporal meanings, that is, they refer to places or locations in the network. Thus, information identifying the "termination" of a call would be the telephone number called, and would not include special information about when one leg of a multi-party calls ends. Finally, Bell Atlantic asserts that party hold, join, or drop information may not be reasonably available to the carrier because conference call capabilities are often provided through equipment that is external to the switch and may even belong to a service provider unrelated to the carrier.[135]

72. TIA states that, while this item is technically feasible, the provision of party hold, join, and drop information in the manner sought by the FBI would require considerable software coding to add additional call processing traps and new messages necessary to report the information. TIA further states that the interim standard already permits LEAs access to party join and drop information, and therefore, the only additional capability LEAs would receive under this punch list item is hold information. TIA contends, however, that such information is not always detected by the switch and even when it is detected, the switch may not have the specific identification information requested by the FBI.[136]

73. DoJ/FBI argue that without party hold, join, and drop information, a LEA often would not know who joins or leaves a conference call, whether the subject alternated between legs of the call, or which parties may have heard or said particular communications during the course of the call. They also contend that we should not use the instant proceeding to determine whether such information is reasonably available to particular carriers or platforms, but should frame an appropriate definition of reasonably available and leave the application of that definition to be worked out by individual carriers and LEAs on a case-by-case basis. DoJ/FBI further argue that the interim standard's Change message[137] is not a substitute for party join information because: (1) the Change message is triggered by changes in *call* identities,[138] rather than by

[135] Bell Atlantic Comments, at 8-11.

[136] TIA Comments, at 29.

[137] The Change message is used to report merging or splitting of connection-oriented call identities. J-STD-025, at § 6.34.

[138] The Call Identity parameter is used to uniquely identify a particular call, call appearance, or call legs within the context of a single system. J-STD-025, at § 6.42.

changes in *party* identities,[139] and therefore will not identify party joins if a manufacturer uses a single call identity to cover multiple legs of a call; (2) the interim standard's Release message[140] is not a proxy for a party drop message because it does not require a carrier to send the Release message when a single call leg or call appearance is released; and (3) the industry has not suggested that the interim standard provides any message that notifies the LEA of party holds.[141] Additionally, DoJ/FBI contend that commenters who oppose this capability err by treating a multi-party, multi-leg call as a single communication because doing so would mean that the LEA in many cases would lack proof of which party participated in a particular conversation and which parties did not. Finally, DoJ/FBI assert that the industry argument that this capability does not exist today confuses the information available to the network and the messages used to encapsulate the information and convey it to the LEA. DoJ/FBI maintain that whether particular information exists in a network is relevant to a carrier's obligations under section 103(a)(2), but that whether a particular message exists is irrelevant to the carrier's obligations.[142]

74. *Discussion.* We find that party hold/join/drop information falls within CALEA's definition of "call-identifying information" because it is "signaling information that identifies the origin, direction, destination, or termination of each communication generated or received" by the subject.[143] Party join information appears to identify the origin of a communication; party drop, the termination of a communication; and party hold, the temporary origin, temporary termination, or re-direction of a communication. This capability also appears to be necessary to enable the LEA to isolate call-identifying and content information because, without it, the LEA would be unable to determine who is talking to whom, and, more accurately, to focus on the subject's role in the conversation.[144] Further, by isolating the call-identifying information in this manner, the LEA can screen out third parties who are not privy to the communications involving the subject, thereby furthering privacy considerations.

---

[139] The Party Identity parameter identifies a party to a call or call attempt. J-STD-025, at § 6.47.

[140] The Release message is used to report that a connection-oriented call has been released. J-STD-025, at § 6.38.

[141] DoJ/FBI Comments, at 45-47.

[142] DoJ/FBI Reply Comments, at 40-41.

[143] Section 102(2) of CALEA, 47 U.S.C. § 1001(2).

[144] We note that Section 103 specifically requires a telecommunications carrier to:

> (a) ensure that its equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of --
>
> (2) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to access call-identifying information that is reasonably available to the carrier --
>
> (B) in a manner that allows it to be associated with the communication to which it pertains.

75. We further find that party hold/join/drop information is reasonably available to the carrier in those cases where the carrier's facilities, equipment or services are involved in providing the service, and that the anticipated costs to carriers of adding this capability are not so exorbitant as to require automatic exclusion of the capability. In percentage terms, based on the manufacturers' aggregate revenue estimates, these costs would be 7% of the core interim standard and 15% of the total punch list.[145] To the extent that CPE is used to provide such features, we conclude that party hold/join/drop information is not reasonably available to the LEA since no network signal would be generated. Thus, we conclude that the provision of party hold, join, and drop information on conference calls, to the extent a network signal is generated, is a technical requirement that meets the assistance capability requirements of section 103.[146]

3. Subject-initiated dialing and signaling information

76. *Background.* This capability would permit the LEA to be informed when a subject using the facilities under surveillance uses services such as call forwarding, call waiting, call hold, and three-way calling. DoJ/FBI requests this information for each communication initiated by the subject. This capability would require the telecommunications carrier to deliver a message to the LEA, informing the LEA that the subject has invoked a feature that would place a party on hold, transfer a call, forward a call, or add/remove a party to a call.

77. The *Further NPRM* tentatively concluded that this capability fits within the definition of call-identifying information and therefore must be provided by the carrier to the LEA where reasonably available.[147] The *Further NPRM* requested comment on whether remote subject-initiated dialing and signaling should affect this tentative conclusion, and noted that to the extent CPE is used to initiate dialing and signaling no information need be provided to the LEA. The five manufacturers' aggregate revenue estimate for this capability is $35 million.[148]

78. *Comments.* SBC and USTA state that subject-initiated dialing and signaling information is not call-identifying and may not be reasonably available.[149] SBC argues that only if the subscriber action can be detected within a CALEA-equipped switch does this feature meet

[145] *See* Appendix B, *infra.*

[146] 47 U.S.C. § 1006(b).

[147] *Further NPRM*, at ¶¶ 91-94.

[148] *See Public Notice*, at 4.

[149] SBC Comments, at 13; USTA Comments, at 15.

the standard, and it is unknown whether a signal of this nature can be incorporated into the switch by manufacturers at a reasonable cost.[150]

79. TIA states that subject-initiated dialing and signaling information has nothing to do with call processing, and that the interim standard generally provides all of the relevant call-identifying information. TIA contends that the only additional information the LEA would receive under this punch list item is the identity of the keys pressed by the subject to enable the feature, and most manufacturers would have to make fairly substantial modifications to their equipment to capture and report such information.[151]

80. BellSouth contends that subject-initiated dialing and signaling information would be redundant with the information provided by party join, hold, and drop messages. BellSouth also states that privacy concerns would be raised by this capability.[152]

81. DoJ/FBI contend that industry's arguments that information about a subject's use of flash hook, feature keys, and similar activity is not call-identifying are incorrect. DoJ/FBI argue that a subject's use of these feature keys changes the connections between the parties to a call, and in so doing changes the "direction" and "destination" (and in some cases "origin" or "termination") of one or more "communication[s] generated or received" by the subject. Moreover, DoJ/FBI argue that any use of feature keys or flash hooks by a subject to control a call constitutes "direction" of the communication by the subject. DoJ/FBI further argue that BellSouth's suggestion that the information a LEA would derive from a subject's dialing and signaling activity is redundant with the information it would learn from party join, hold, drop messages is incorrect because dialing and signaling may be either pre- or post-cut-through, and may be transmitted either in- or out-of-band. DoJ/FBI states that some of this activity may result in party joins, holds, or drops, but much of it will not; and that, conversely, there will be many instances in which a change in party connections does not reflect any subject-initiated dialing and signaling activity.[153]

82. *Discussion.* We conclude that subject-initiated dialing and signaling information fits within the definition of call-identifying information contained in section 102(2) of CALEA, and that the anticipated costs to carriers of adding this capability are not so exorbitant as to require automatic exclusion of the capability. In percentage terms, based on the manufacturers'

[150] SBC Comments, at 13-14.

[151] TIA Comments, at 30-32.

[152] BellSouth Comments, at 16.

[153] DoJ/FBI Reply Comments, at 44-47.